CLAIMS

1. An enforcement architecture for digital rights management, wherein the architecture enforces rights in protected digital content, the architecture comprising:

a content server for distributing the digital content;

a license server for issuing at least one digital license corresponding to and separate from the digital content; and

a computing device for receiving the distributed digital content and for receiving and storing any digital license corresponding to the digital content, the computing device having:

a rendering application for rendering the digital content; and

a Digital Rights Management (DRM) system for being invoked by the rendering application upon such rendering application attempting to render the digital content, the DRM system for determining whether a right to render the digital content in the manner sought exists based on any digital license stored in the computing device and corresponding to the digital content.

2. The architecture of claim 1, wherein the content server is communicatively coupled to a network and distributes the digital content over the network.

3. The architecture of claim 2, wherein the content server is communicatively coupled to the Internet and distributes the digital content over the Internet.

4. The architecture of claim 1, wherein the license server is communicatively coupled to a network and issues the at least one digital license over the network.

5. The architecture of claim 4, wherein the license server is communicatively coupled to the Internet and issues the at least one digital license over the Internet.

6. The architecture of claim 1, wherein the content server is communicatively coupled to a portable medium writer and distributes the digital content on a portable medium written by the portable medium writer, the portable medium selected from the group consisting of an optical storage medium and a magnetic storage medium.

7. The architecture of claim 1, wherein the content server distributes the digital content in an encrypted form.

8. The architecture of claim 7, wherein each digital license corresponding to the digital content includes:

a decryption key that decrypts the encrypted digital content; and

a description of the rights conferred by the license, wherein the encrypted digital content cannot be decrypted and rendered without obtaining such license from the license server.

9. The architecture of claim 8, wherein each digital license corresponding to the digital content further includes a digital signature that binds the license to the encrypted digital content.

10. The architecture of claim 1, wherein if the DRM system determines that the right to render the digital content in the manner sought does not exist based on any digital license stored in the computing device and corresponding to the digital content, such DRM system directs a computing device user to the license server to obtain a digital license to render such digital content in the manner sought.

11. The architecture of claim 1, wherein if the DRM system determines that the right to render the digital content in the manner sought does not exist based on any digital license stored in the computing device and corresponding to the digital content, such DRM system transparently obtains a digital license from the license server without any action necessary on the part of a computing device user.

12. The architecture of claim 1, wherein the DRM system includes a license store for storing digital licenses.

13. The architecture of claim 1, wherein each digital license corresponding to the digital content is bound to such digital content.

14. The architecture of claim 13, wherein each digital license corresponding to the digital content is bound to such digital content by way of a public / private key technique.

15. The architecture of claim 1, wherein the license server issues a digital license to a DRM system only if the license server trusts such DRM system to abide by the license.

16. The architecture of claim 15, wherein the content server distributes the digital content in an encrypted form, and wherein the DRM system includes a trusted black box for performing decryption and encryption functions for such DRM system.

17. The architecture of claim 16, wherein the black box includes a unique public / private key pair for performing the decryption and encryption functions.

18. The architecture of claim 17, wherein the license server issues each digital license in response to a license request from the DRM system, the license request including the black box public key, the license server encrypting at least a portion of the

digital license according to the black box public key prior to issuance of such license, thereby binding such license to such black box.

19. The architecture of claim 18, wherein the content server distributes the digital content in an encrypted form, wherein each digital license corresponding to the digital content includes a decryption key that decrypts the encrypted digital content, and wherein the license server encrypts the decryption key in the license according to the black box public key.

20. The architecture of claim 19, wherein each digital license corresponding to the digital content further includes a description of the rights conferred by the license, wherein the encrypted digital content cannot be decrypted and rendered without obtaining such license from the license server, and wherein the license server encrypts the rights description in the license according to the decryption key.

21. The architecture of claim 16, wherein the black box includes a version number.

22. The architecture of claim 21 wherein the license server issues each digital license in response to a license request from the DRM system, the license request including the version number of the black box, the license server determining prior to issuance of the license whether the version number of the black box is acceptable, the license server upon determining that the version number of the black box is not acceptable refusing to issue the license until the black box is updated, the architecture further comprising a black box server for providing an updated black box to the DRM system.

23. The architecture of claim 16, wherein the black box includes a certifying authority signature as provided by an approved certifying authority.

24. The architecture of claim 23 wherein the license server issues each

digital license in response to a license request from the DRM system, the license request including the certifying authority signature, the license server determining prior to issuance of the license whether the certifying authority signature is valid.

25. The architecture of claim 15, wherein each digital license corresponding to the digital content includes a description of the rights conferred by the license, and wherein the DRM system includes a trusted license evaluator for evaluating the rights description and allowing rendering of the digital content by the rendering application only if such rendering is in accordance with the rights description of the license.

26. The architecture of claim 1 further comprising an issued license database for maintaining information on digital licenses issued by the license server, wherein if the computing device loses a received license, a re-issue thereof may be provided based on the information in the issued license database.

27. The architecture of claim 1 further comprising an authoring tool for authoring the digital content distributed by the content server in a form amenable to the architecture.

28. The architecture of claim 27 wherein the authoring tool encrypts the digital content according to a decryption key and stores information on the digital content and the encryption key in a content-key database.

29. The architecture of claim 28 wherein the license server accesses the information on the digital content and the encryption key in the content-key database prior to issuance of a license corresponding to the digital content, and includes the decryption key with such license as issued.

30. A method for implementing digital rights management, wherein the

method enforces rights in protected digital content, the method comprising:

distributing the digital content from a content server to a computing device of a user;

receiving the distributed digital content at the computing device;

attempting to render the digital content by way of a rendering application;

invoking, by the rendering application, a Digital Rights Management (DRM) system upon such rendering application attempting to render the digital content;

determining, by the DRM system, whether a right to render the digital content in the manner sought exists based on any digital license stored in the computing device and corresponding to the digital content; and

if the right does not exist:

requesting from a license server a digital license that provides such right and that corresponds to and is separate from the digital content;

issuing, by the license server, the digital license to the DRM system;

receiving, by the computing device, the issued digital license corresponding to the digital content from the license server; and

storing the received digital license on the computing device.

31. The method of claim 30, wherein the distributing step comprises distributing the digital content over a network.

32. The method of claim 31, wherein the distributing step comprises distributing the digital content over the Internet.

33. The method of claim 30, wherein the issuing step comprises issuing the digital license over a network.

34. The method of claim 33, wherein the issuing step comprises issuing the digital license over the Internet.

35. The method of claim 30, wherein the distributing step comprises distributing the digital content on a portable medium selected from the group consisting of an optical storage medium and a magnetic storage medium.

36. The method of claim 30, wherein the distributing step comprises distributing the digital content in an encrypted form.

37. The method of claim 36, further comprising including with each digital license corresponding to the digital content:

a decryption key that decrypts the encrypted digital content; and

a description of the rights conferred by the license, wherein the encrypted digital content cannot be decrypted and rendered without obtaining such license from the license server.

38. The method of claim 37, wherein the including step further comprises including with each digital license corresponding to the digital content a digital signature that binds the license to the encrypted digital content.

39. The method of claim 30, wherein the requesting a digital license step comprises directing, by the DRM system, a computing device user to the license server to obtain a digital license to render such digital content in the manner sought.

40. The method of claim 30, wherein the requesting a digital license step comprises transparently obtaining, by the DRM system, a digital license from the license server without any action necessary on the part of a computing device user.

41. The method of claim 30, wherein the storing step comprises storing,

by the DRM system, the received digital license in a license store of the DRM system.

42. The method of claim 30, further comprising binding, by the license server, the digital license to the corresponding digital content.

43. The method of claim 42, comprising binding, by the license server, the digital license to the corresponding digital content by way of a public / private key technique.

44. The method of claim 30, wherein the issuing step comprises issuing, by the license server, the digital license to the DRM system only if the license server trusts such DRM system to abide by the license.

45. The method of claim 44, wherein the distributing step comprises distributing, by the content server, the digital content in an encrypted form, and further comprising employing a trusted black box in the DRM system to perform decryption and encryption functions for such DRM system.

46. The method of claim 45, wherein the black box includes a public / private key pair, and wherein the requesting a digital license step comprises including in the request the black box public key, and further comprising encrypting, by the license server, at least a portion of the digital license according to the black box public key prior to issuance of such license, thereby binding such license to such black box.

47. The method of claim 46, wherein the distributing step comprises distributing the digital content in an encrypted form, and further comprising:

including with each digital license corresponding to the digital content a decryption key that decrypts the encrypted digital content; and

encrypting, by the license server, the decryption key in the license according to the black box public key.

48. The method of claim 47, further comprising:

including with each digital license corresponding to the digital content a description of the rights conferred by the license, wherein the encrypted digital content cannot be decrypted and rendered without obtaining such license from the license server; and

encrypting, by the license server, the rights description in the license according to the decryption key.

49. The method of claim 45, wherein the black box includes a version number, and wherein the requesting a digital license step comprises including in the request the version number of the black box, and further comprising:

determining, by the license server, prior to issuance of the license whether the version number of the black box is acceptable; and

upon determining that the version number of the black box is not acceptable, the license server refusing to issue the license until the black box is updated, the architecture further comprising a black box server for providing an updated black box to the DRM system.

50. The method of claim 45, wherein the black box includes a certifying authority signature as provided by an approved certifying authority, and wherein the requesting a digital license step comprises including the certifying authority signature, the license server determining prior to issuance of the license whether the certifying authority signature is valid.

51. The method of claim 44, wherein the issuing the digital license step comprises including with the digital license a description of the rights conferred by the license, and further comprising:

evaluating, by a trusted license evaluator of the DRM system, the rights description; and

allowing rendering of the digital content by the rendering application only if such rendering is in accordance with the rights description of the license.

52. The method of claim 30 further comprising maintaining information on digital licenses issued by the license server in an issued license database, wherein if the computing device loses a received license, a re-issue thereof may be provided based on the information in the issued license database.

53. The method of claim 30 further comprising authoring, by an authoring tool, the digital content distributed by the content server in a form amenable to the architecture.

54. The method of claim 53 wherein the authoring step comprises:

encrypting the digital content according to a decryption key; and

storing information on the digital content and the encryption key in a content-key database.

55. The method of claim 54 wherein the issuing the digital license step comprises:

accessing, by the license server, the information on the digital content and the encryption key in the content-key database prior to issuance of a license corresponding to the digital content; and

including the decryption key with such license as issued.

56. An enforcement architecture for digital rights management, wherein the architecture enforces rights in protected digital content, the architecture comprising:

a content server communicatively coupled to a network for distributing the digital content over the network;

a license server for issuing at least one digital license corresponding to and separate from the digital content, the license server being communicatively coupled to the network for issuing the at least one digital license over the network; and

a computing device communicatively coupled to the network for receiving the distributed digital content and for receiving any digital license corresponding to the digital content, the computing device also having:

a memory for storing any digital license corresponding to the digital content;

a rendering application for attempting to render the digital content; and

a Digital Rights Management (DRM) system for being invoked by the rendering application upon such rendering application attempting to render the digital content, the DRM system for determining whether a right to render the digital content in the manner sought exists based on any digital license stored in the computing device and corresponding to the digital content.

57. The architecture of claim 56, wherein the content server is communicatively coupled to the Internet and distributes the digital content over the Internet.

58. The architecture of claim 56, wherein the license server is communicatively coupled to the Internet and issues the at least one digital license over the Internet.

59. The architecture of claim 56, wherein the content server is also communicatively coupled to a portable medium writer and distributes the digital content on a portable medium written by the portable medium writer, the portable medium selected from the group consisting of an optical storage medium and a magnetic storage medium, and wherein the computing device includes a portable medium reader corresponding to the portable medium writer for receiving and reading the portable medium.

60. The architecture of claim 56, wherein the content server distributes the digital content in an encrypted form.

61. The architecture of claim 60, wherein each digital license corresponding to the digital content includes:

a decryption key that decrypts the encrypted digital content; and

a description of the rights conferred by the license, wherein the encrypted digital content cannot be decrypted and rendered without obtaining such license from the license server.

62. The architecture of claim 61, wherein each digital license corresponding to the digital content further includes a digital signature that binds the license to the encrypted digital content.

63. The architecture of claim 56, wherein if the DRM system determines that the right to render the digital content in the manner sought does not exist based on any digital license stored in the computing device and corresponding to the digital content, such DRM system directs a computing device user to the license server to obtain a digital license to render such digital content in the manner sought.

64. The architecture of claim 56, wherein if the DRM system determines that the right to render the digital content in the manner sought does not exist based on any digital license stored in the computing device and corresponding to the

digital content, such DRM system transparently obtains a digital license from the license server without any action necessary on the part of a computing device user.

65. The architecture of claim 56, wherein the DRM system includes a license store for storing digital licenses.

66. The architecture of claim 56, wherein each digital license corresponding to the digital content is bound to such digital content.

67. The architecture of claim 66, wherein each digital license corresponding to the digital content is bound to such digital content by way of a public / private key technique.

68. The architecture of claim 56, wherein the license server issues a digital license to a DRM system only if the license server trusts such DRM system to abide by the license.

69. The architecture of claim 68, wherein the content server distributes the digital content in an encrypted form, and wherein the DRM system includes a trusted black box for performing decryption and encryption functions for such DRM system.

70. The architecture of claim 69, wherein the black box includes a unique public / private key pair for performing the decryption and encryption functions.

71. The architecture of claim 70, wherein the license server issues each digital license in response to a license request from the DRM system, the license request including the black box public key, the license server encrypting at least a portion of the digital license according to the black box public key prior to issuance of such license, thereby binding such license to such black box.

72. The architecture of claim 71, wherein the content server distributes the digital content in an encrypted form, wherein each digital license corresponding to the digital content includes a decryption key that decrypts the encrypted digital content, and wherein the license server encrypts the decryption key in the license according to the black box public key.

73. The architecture of claim 72, wherein each digital license corresponding to the digital content further includes a description of the rights conferred by the license, wherein the encrypted digital content cannot be decrypted and rendered without obtaining such license from the license server, and wherein the license server encrypts the rights description in the license according to the decryption key.

74. The architecture of claim 69, wherein the black box includes a version number.

75. The architecture of claim 74 wherein the license server issues each digital license in response to a license request from the DRM system, the license request including the version number of the black box, the license server determining prior to issuance of the license whether the version number of the black box is acceptable, the license server upon determining that the version number of the black box is not acceptable refusing to issue the license until the black box is updated, the architecture further comprising a black box server for providing an updated black box to the DRM system.

76. The architecture of claim 69, wherein the black box includes a certifying authority signature as provided by an approved certifying authority.

77. The architecture of claim 76 wherein the license server issues each digital license in response to a license request from the DRM system, the license request including the certifying authority signature, the license server determining prior to issuance of the license whether the certifying authority signature is valid.

78. The architecture of claim 68, wherein each digital license corresponding to the digital content includes a description of the rights conferred by the license, and wherein the DRM system includes a trusted license evaluator for evaluating the rights description and allowing rendering of the digital content by the rendering application only if such rendering is in accordance with the rights description of the license.

79. The architecture of claim 56 further comprising an issued license database for maintaining information on digital licenses issued by the license server, wherein if the computing device loses a received license, a re-issue thereof may be provided based on the information in the issued license database.

80. The architecture of claim 56 further comprising an authoring tool for authoring the digital content distributed by the content server in a form amenable to the architecture.

81. The architecture of claim 80 wherein the authoring tool encrypts the digital content according to a decryption key and stores information on the digital content and the encryption key in a content-key database.

82. The architecture of claim 81 wherein the license server accesses the information on the digital content and the encryption key in the content-key database prior to issuance of a license corresponding to the digital content, and includes the decryption key with such license as issued.

83. An enforcement architecture for digital rights management, wherein the architecture enforces rights in protected digital content, the architecture comprising:

an authoring tool for authoring the digital content in a form amenable to the architecture;

a content server for receiving the digital content from the authoring tool and distributing the digital content; and

a license server for issuing at least one digital license corresponding to and separate from the digital content, wherein a computing device receives the distributed digital content and receives and stores any digital license corresponding to the digital content, the computing device having a rendering application for rendering the digital content; and a Digital Rights Management (DRM) system for being invoked by the rendering application upon such rendering application attempting to render the digital content, the DRM system for determining whether a right to render the digital content in the manner sought exists based on any digital license stored in the computing device and corresponding to the digital content.

84. The architecture of claim 83, wherein the content server is communicatively coupled to a network and distributes the digital content over the network.

85. The architecture of claim 84, wherein the content server is communicatively coupled to the Internet and distributes the digital content over the Internet.

86. The architecture of claim 83, wherein the license server is communicatively coupled to a network and issues the at least one digital license over the network.

87. The architecture of claim 86, wherein the license server is communicatively coupled to the Internet and issues the at least one digital license over the Internet.

88. The architecture of claim 83, wherein the content server is communicatively coupled to a portable medium writer and distributes the digital content on a portable medium written by the portable medium writer, the portable medium selected

from the group consisting of an optical storage medium and a magnetic storage medium.

89. The architecture of claim 1, wherein the content server distributes the digital content in an encrypted form.

90. The architecture of claim 89, wherein each digital license corresponding to the digital content includes:

a decryption key that decrypts the encrypted digital content; and

a description of the rights conferred by the license, wherein the encrypted digital content cannot be decrypted and rendered without obtaining such license from the license server.

91. The architecture of claim 90, wherein each digital license corresponding to the digital content further includes a digital signature that binds the license to the encrypted digital content.

92. The architecture of claim 83, wherein a computing device user is directed to the license server by the DRM system to obtain a digital license to render the digital content in the manner sought if the DRM system determines that the right to render such digital content in the manner sought does not exist based on any digital license stored in the computing device and corresponding to the digital content.

93. The architecture of claim 83, wherein the DRM system transparently obtains a digital license from the license server without any action necessary on the part of a computing device user if the DRM system determines that the right to render the digital content in the manner sought does not exist based on any digital license stored in the computing device and corresponding to the digital content.

94. The architecture of claim 83, wherein each digital license corresponding to the digital content is bound to such digital content.

95. The architecture of claim 94, wherein each digital license corresponding to the digital content is bound to such digital content by way of a public / private key technique.

96. The architecture of claim 83, wherein the license server issues a digital license to a DRM system only if the license server trusts such DRM system to abide by the license.

97. The architecture of claim 96, wherein the content server distributes the digital content in an encrypted form, wherein the DRM system includes a trusted black box for performing decryption and encryption functions for such DRM system, wherein the black box includes a unique public / private key pair for performing the decryption and encryption functions, and wherein the license server issues each digital license in response to a license request from the DRM system, the license request including the black box public key, the license server encrypting at least a portion of the digital license according to the black box public key prior to issuance of such license, thereby binding such license to such black box.

98. The architecture of claim 97, wherein the content server distributes the digital content in an encrypted form, wherein each digital license corresponding to the digital content includes a decryption key that decrypts the encrypted digital content, and wherein the license server encrypts the decryption key in the license according to the black box public key.

99. The architecture of claim 98, wherein each digital license corresponding to the digital content further includes a description of the rights conferred by the license, wherein the encrypted digital content cannot be decrypted and rendered without obtaining such license from the license server, and wherein the license server encrypts the rights description in the license according to the decryption key.

100. The architecture of claim 97, wherein the black box includes a version number, and wherein the license server issues each digital license in response to a license request from the DRM system, the license request including the version number of the black box, the license server determining prior to issuance of the license whether the version number of the black box is acceptable, the license server upon determining that the version number of the black box is not acceptable refusing to issue the license until the black box is updated, the architecture further comprising a black box server for providing an updated black box to the DRM system.

101. The architecture of claim 97, wherein the black box includes a certifying authority signature as provided by an approved certifying authority, and wherein the license server issues each digital license in response to a license request from the DRM system, the license request including the certifying authority signature, the license server determining prior to issuance of the license whether the certifying authority signature is valid.

102. The architecture of claim 96, wherein each digital license corresponding to the digital content includes a description of the rights conferred by the license, and wherein the DRM system includes a trusted license evaluator for evaluating the rights description and allowing rendering of the digital content by the rendering application only if such rendering is in accordance with the rights description of the license.

103. The architecture of claim 83 further comprising an issued license database for maintaining information on digital licenses issued by the license server, wherein if the computing device loses a received license, a re-issue thereof may be provided based on the information in the issued license database.

104. The architecture of claim 83 wherein the authoring tool encrypts the

digital content according to a decryption key and stores information on the digital content and the encryption key in a content-key database.

105. The architecture of claim 104 wherein the license server accesses the information on the digital content and the encryption key in the content-key database prior to issuance of a license corresponding to the digital content, and includes the decryption key with such license as issued.

Add A2